Sítě, ochrana komunikace

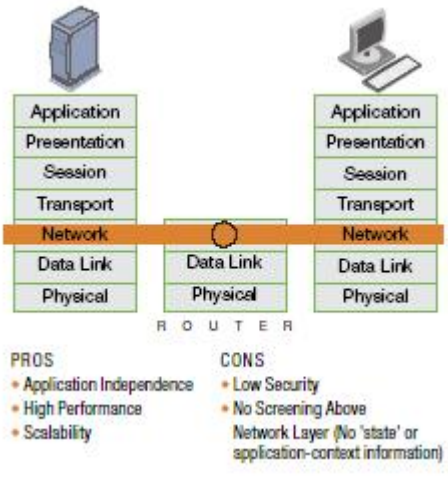
traditional enterprise perimeter has expanded, or effectively disappeared in some cases. Mobile devices like laptops, PDAs, and USB memory sticks constantly travel from one side of the "perimeter" to the other. Wireless LANs allow external connections that bypass firewalls

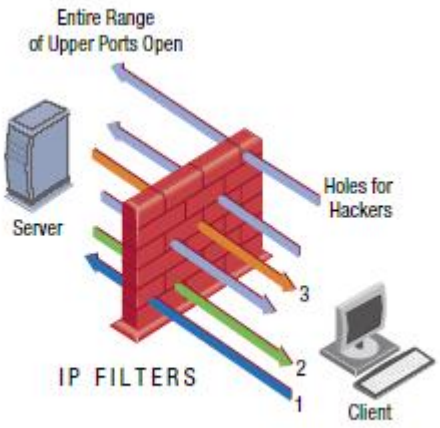
HoneyPot, HoneyNet
ideální prostředí pro útočníka

ochrana síťového perimetru – úplně první problém

Firewally

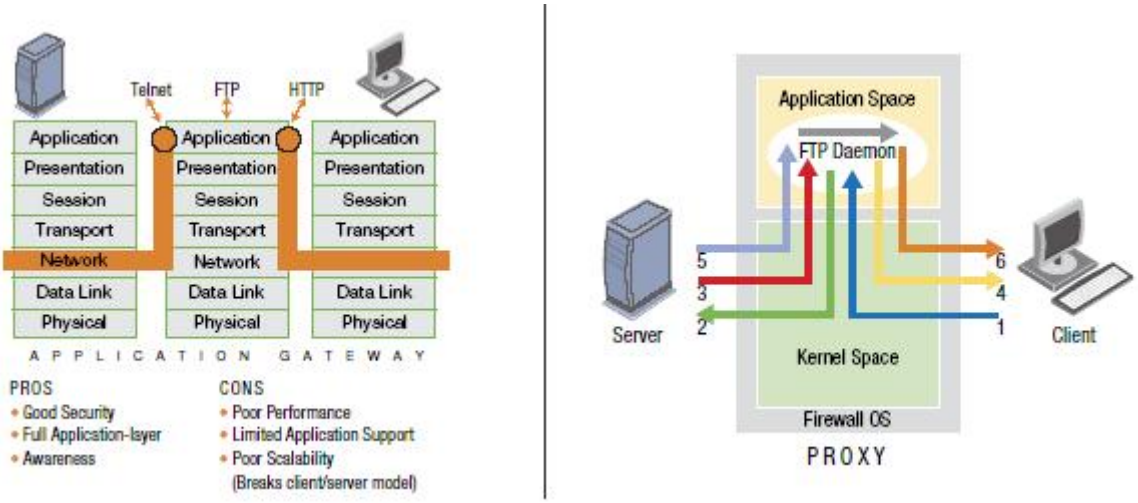
ip filtry (stavové, bezestavové)





aplikační firewally (proxy brány)

musí existovat specializovaná „proxy“ pro každý přenášený protokol
generické proxy zpravidla nedělají nic jiného než tcp forwarding



personální firewally

většinou filtry

Content filtry, proxy servery

provádějí aplikační analýzu dat
odstraňují nežádoucí objekty (skripty, dokumenty, ...)
hodnocení obsahu pro účely zpřístupňování uživatelům

- výměna protokolu mezi zónami
- změna adresace (NAT)

Síťové IDS, IPS

hlídá známe vzory chování odpovídající útoku
IPS může přímo reagovat a proaktivně bránit útoku, IDS detekuje a může vyvolat alert, který případně spustí (externí) bezpečnostní mechanismus

Další nástroje a postupy

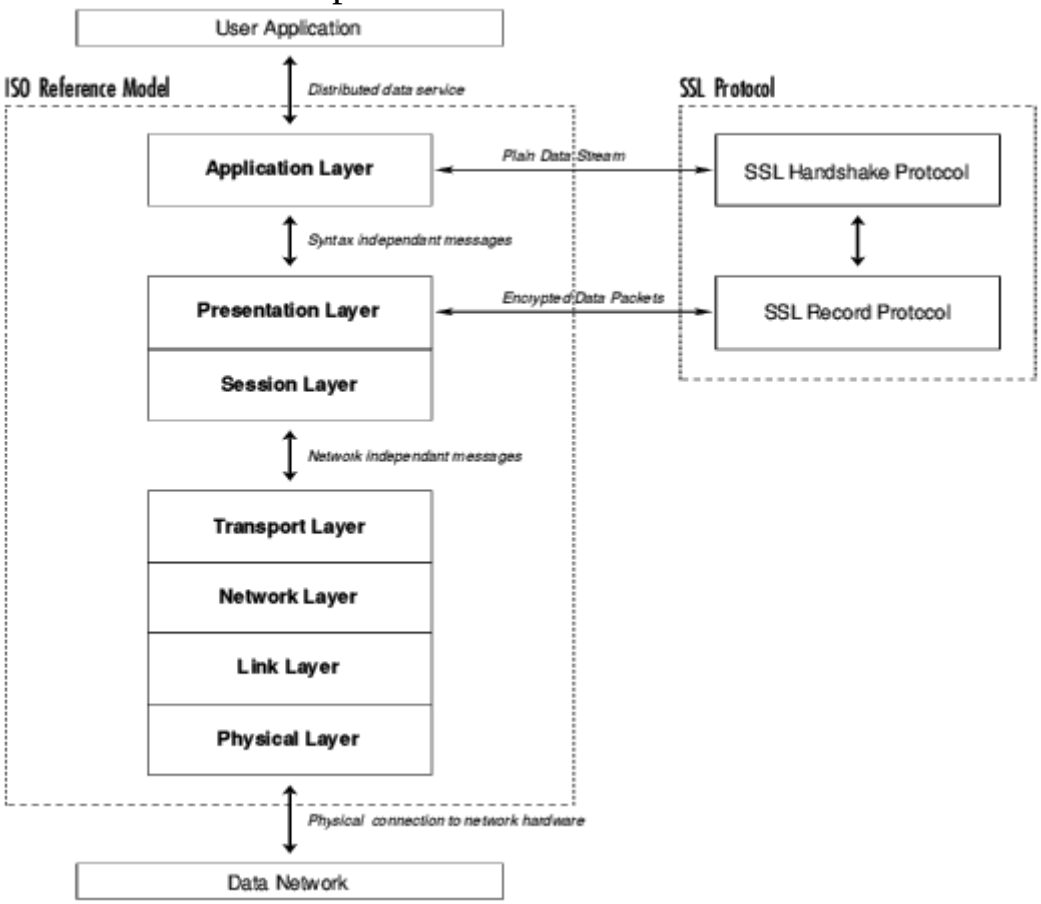
- tunelování
- aplikační šifrování
- anonymita
- **patche**

HW a linkové šifrování

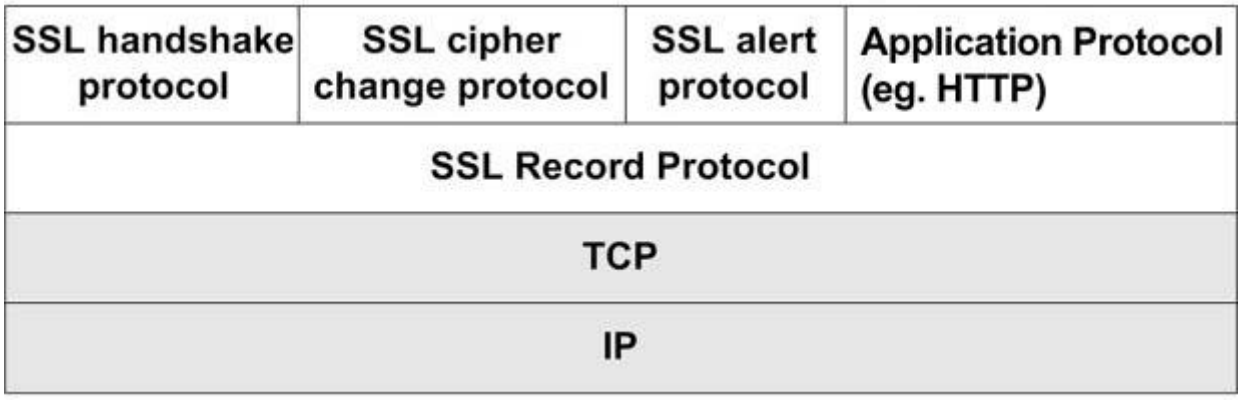
Ochrana komunikace – (sub)aplikační šifrovací protokoly

SSL

místo SSL v rámci protokolového stacku



Struktura SSL



SSL handshake protocol

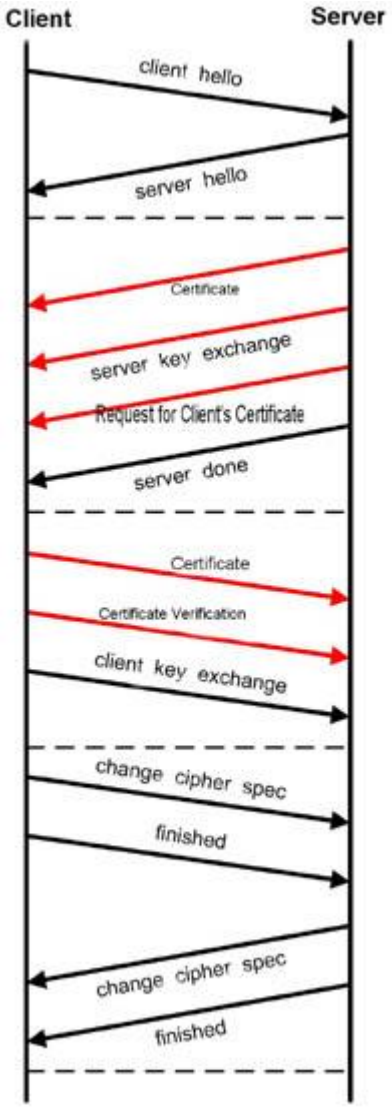
Autentizace serveru

Message Type	Direction	Data Transferred
client-hello	C > S	challenge-data, cipher-specs
server-hello	C < S	connection-id, server-certificate,

		cipher-specs
client-master-key	C > S	cipher-kind, clear-master-key, {secret-master-key}server-public-key
client-finish	C > S	{connection-id}client-write-key
server-verify	C < S	{challenge-data}server-write-key
server-finish	C < S	{session-id}server-write-key

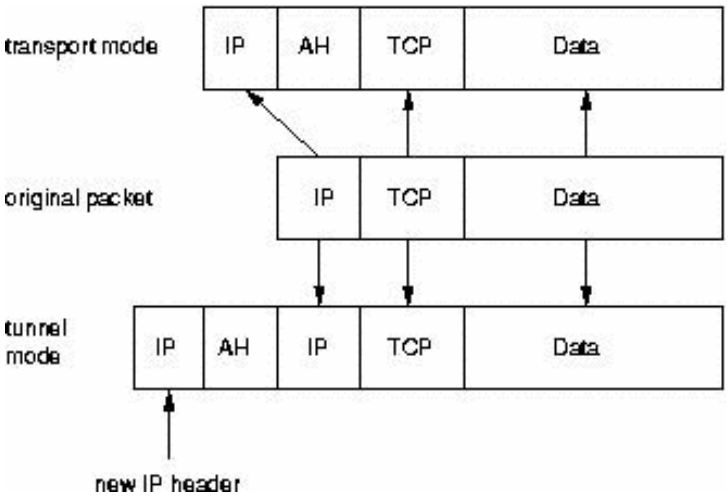
Autentizace klienta

Message Type	**Direction**	**Data Transferred**
client-hello	C > S	challenge-data, session-id, cipher-specs
server-hello	C < S	connection-id, session-id-hit
client-finish	C > S	{connection-id}client-write-key
server-verify	C < S	{challenge-data}server-write-key
request-certificate	C < S	{auth-type, cert-chal-data}server-write-key
client-certificate	C > S	{cert-type, client-cert, resp-data}client-write-key
server-finish	C < S	{session-id}server-write-key



Z protokolu SSL vychází protocol TLS (Microsoft), který je nekompatibilním rozšířením SSL.

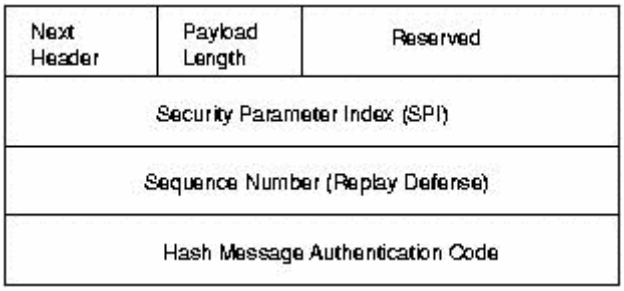
IpSec



IPsec je ve skutečnosti dvojicí nezávislých protokolů: Authentication Header (AH) a Encapsulated Security Payload (ESP)

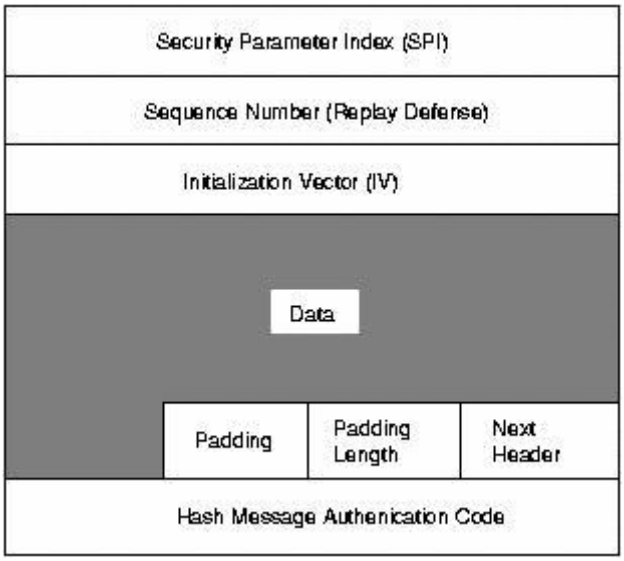
Pracuje ve dvou rozdílných módech (tunnel mode a transport mode)

AH protokol



zajišťuje integritu paketů
počítá se klíčem řízený HMAC z aplikačních dat a konstatních částí hlavičky datagramu (založeno na MD5, SHA1)

ESP protokol



zajišťuje integritu i utajení přenášených dat
pro integritu se opět používá HMAC
pro šifrování se využívají symetrické blokové šifry (*DES*, 3DES, AES, Blowfish, ...)

IpSec sám neřeší key-management

červy, viry

procesory umí nově označit executable segment a nespustí kód z jiného segmentu

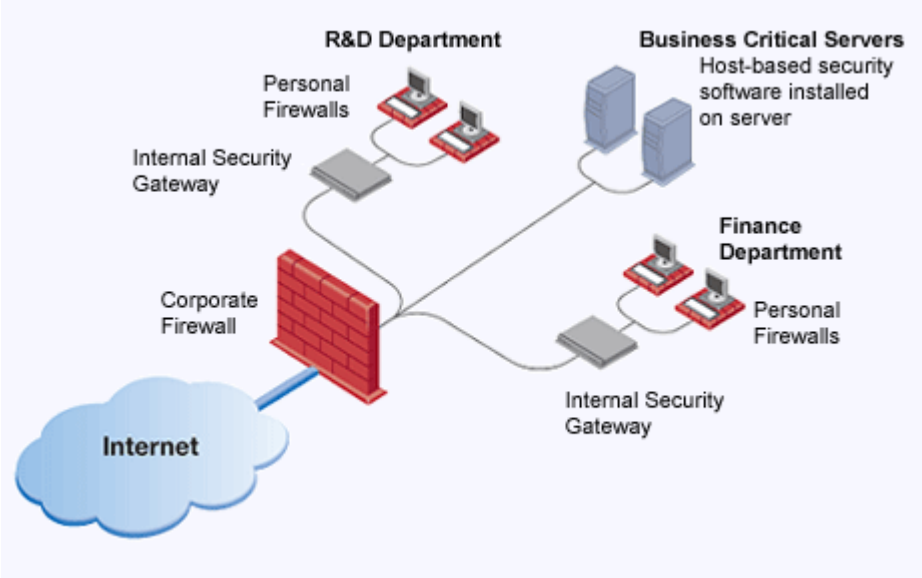
Interní bezpečnost

zákazníci, partneři, konzultanti, ... přistupují ke zdrojům interní sítě
employee with a laptop who works offsite and then plugs the laptop directly into the corporate network
intentional hacking by legitimate and authorized internal users

Internal Security Gateway (ISG)

- Ověřuje soulad se standardy
- Kontroluje použití očekávaných mechanismů
- Hlídá hazardní operace aplikací
- Analyzuje a blokuje nebezpečný spustitelný kód v síťové komunikace

ISG would be placed inline between all traffic into and out of the security zone. Zones can be physical or virtual, and examples include departments in an organization, floors of a building, or all wirelesss access points



Bezpečnost počítačů (end-point)

checks. "Enterprise-ready" means that an administrator can centrally configure and deploy security policy to multiple end-points. Many personal firewalls

critical that end-point security be "enterprise-ready" in terms of flexible policy setting, administration, and ability to ensure conformance to policy via integrity

Internal segmentation (e.g., using routers, switches, and virtual LAN technology) supports logically or physically separating resources that require different levels of security.